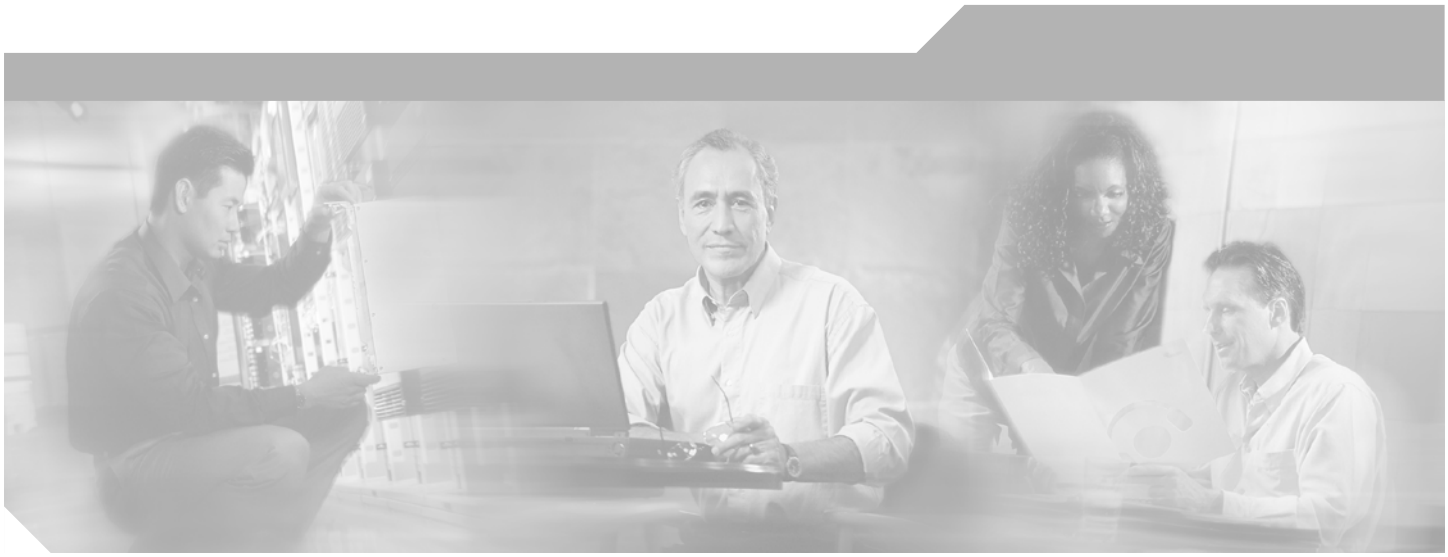


Cisco Catalyst Blade Switch 3030 Hardware Installation Guide

March 2006

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-8389-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

• Turn the television or radio antenna until the interference stops.

• Move the equipment to one side or the other of the television or radio.

• Move the equipment farther away from the television or radio.

• Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco Catalyst Blade Switch 3030 Hardware Installation Guide
© 2006 Cisco Systems, Inc. All rights reserved.

Preface vii

Audience vii

Purpose vii

Organization vii

Conventions viii

Statement 1071—Warning Definition viii

Related Publications xiii

Obtaining Documentation xiv

Cisco.com xiv

Product Documentation DVD xiv

Ordering Documentation xv

Documentation Feedback xv

Cisco Product Security Overview xv

Reporting Security Problems in Cisco Products xvi

Obtaining Technical Assistance xvi

Cisco Technical Support & Documentation Website xvi

Submitting a Service Request xvii

Definitions of Service Request Severity xvii

Obtaining Additional Publications and Information xviii

CHAPTER 1

Product Overview 1-1

Features 1-1

Front Panel Description 1-2

Switch Console Port 1-2

10/100/1000 Ports 1-3

SFP Module Slots 1-3

LEDs 1-4

System Status/ID LED 1-4

Console Port LEDs 1-4

Port LEDs 1-5

Rear Panel Description 1-5

Power Connectors 1-5

Management Options 1-6
Using the Device Manager 1-6
Using the Command-Line Interface 1-7
Using SNMP 1-7
Network Configurations 1-7

CHAPTER 2 **Switch Installation** 2-1
Preparing for Installation 2-1
Warnings 2-1
Installation Guidelines 2-3
Verifying Package Contents 2-4
Dell Modular Server Chassis Architecture 2-5
Installing the Switch Module into the Server Chassis 2-6
Configuring the Switch Module 2-7
Connecting through the Switch Module Console Port 2-8
Connecting through the DRAC/MC 2-9
Waiting for POST to Complete 2-11
Completing the Initial Configuration 2-11
Installing and Removing SFP Modules 2-13
Installing SFP Modules into SFP Module Slots 2-14
Removing SFP Modules from SFP Module Slots 2-15
Connecting to the 10/100/1000 Ports 2-16
Connecting to SFP Modules 2-17
Connecting to Fiber-Optic SFP Modules 2-17
Connecting to 1000BASE-T SFP Modules 2-18
Where to Go Next 2-19

CHAPTER 3 **Troubleshooting** 3-1
Understanding POST Results 3-1
Diagnosing Problems 3-1

APPENDIX A **Technical Specifications** A-1

APPENDIX B **Connector and Cable Specifications** B-1
Connector Specifications B-1
10/100/1000 Ports B-1
Connecting to 10BASE-T- and 100BASE-TX-Compatible Devices B-1
Connecting to 1000BASE-T Devices B-2

SFP Module Ports B-3
Console Port B-3
Cable and Adapter Specifications B-4
Two Twisted-Pair Cable Pinouts B-4
Four Twisted-Pair Cable Pinouts for 1000BASE-T Ports B-4
Crossover Cable and Adapter Pinouts B-5
Identifying a Crossover Cable B-5
Adapter Pinouts B-6

APPENDIX C **Configuring the Switch with the CLI-Based Setup Program** C-1
Accessing the CLI Through the Console Port C-1
Taking Out What You Need C-1
Connecting to the Console Port C-2
Completing the Initial Configuration C-4

INDEX

Preface

Audience

This guide is for the networking or computer technician responsible for installing the Cisco Catalyst Blade Switch 3030—also referred to as *the switch*—into the Dell Modular Server Chassis—also referred to as *the server chassis.* We assume that you are familiar with the concepts and terminology of Ethernet and local area networking.

Purpose

This guide describes the hardware features of the Cisco Catalyst Blade Switch 3030. It describes the physical and performance characteristics of the switch, explains how to install it, and provides troubleshooting information.

This guide does not describe system messages that you might receive or how to configure your switch. For more information, refer to the switch software configuration guide, the switch command reference, and the switch system message guide on the Cisco.com Product Documentation home page. For information about the standard Cisco IOS Release 12.1 commands, refer to the Cisco IOS documentation set from the Cisco.com home page at **Service and Support > Technical Documents.** On the Cisco Product Documentation home page, select Release **12.1** from the Cisco IOS Software drop-down list.

Organization

This guide is organized into these chapters:

Chapter 1, "Product Overview," is a physical and functional overview of the switch module. It describes the switch ports, the standards they support, and the switch LEDs.

Chapter 2, "Switch Installation," contains the procedures on how to install the switch in the server chassis and how to make port connections.

Chapter 3, "Troubleshooting," describes how to identify and resolve some of the problems that might arise when installing the switch.

Appendix A, "Technical Specifications," lists the physical and environmental specifications for the switches and the regulatory agency approvals.

Appendix B, "Connector and Cable Specifications," describes the connectors, cables, and adapters that can be used to connect to the switch.

Appendix C, "Configuring the Switch with the CLI-Based Setup Program," has an installation and setup procedure for a standalone switch.

Conventions

This document uses these conventions and symbols for notes, cautions, and warnings:

Note Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Statement 1071—Warning Definition

Warning **IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Waarschuwing **BELANGRIJKE VEILIGHEIDSINSTRUCTIES**

Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van de standaard praktijken om ongelukken te voorkomen. Gebruik het nummer van de verklaring onderaan de waarschuwing als u een vertaling van de waarschuwing die bij het apparaat wordt geleverd, wilt raadplegen.

BEWAAR DEZE INSTRUCTIES

Varoitus **TÄRKEITÄ TURVALLISUUSOHJEITA**

Tämä varoitusmerkki merkitsee vaaraa. Tilanne voi aiheuttaa ruumiillisia vammoja. Ennen kuin käsittelet laitteistoa, huomioi sähköpiirien käsittelemiseen liittyvät riskit ja tutustu onnettomuuksien yleisiin ehkäisytapoihin. Turvallisuusvaroitusten käännökset löytyvät laitteen mukana toimitettujen käännettyjen turvallisuusvaroitusten joukosta varoitusten lopussa näkyvien lausuntonumeroiden avulla.

SÄILYTÄ NÄMÄ OHJEET

Attention **IMPORTANTES INFORMATIONS DE SÉCURITÉ**

Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers liés aux circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions des avertissements figurant dans les consignes de sécurité traduites qui accompagnent cet appareil, référez-vous au numéro de l'instruction situé à la fin de chaque avertissement.

CONSERVEZ CES INFORMATIONS

Warnung **WICHTIGE SICHERHEITSHINWEISE**

Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu Verletzungen führen kann. Machen Sie sich vor der Arbeit mit Geräten mit den Gefahren elektrischer Schaltungen und den üblichen Verfahren zur Vorbeugung vor Unfällen vertraut. Suchen Sie mit der am Ende jeder Warnung angegebenen Anweisungsnummer nach der jeweiligen Übersetzung in den übersetzten Sicherheitshinweisen, die zusammen mit diesem Gerät ausgeliefert wurden.

BEWAHREN SIE DIESE HINWEISE GUT AUF.

Avvertenza **IMPORTANTI ISTRUZIONI SULLA SICUREZZA**

Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di intervenire su qualsiasi apparecchiatura, occorre essere al corrente dei pericoli relativi ai circuiti elettrici e conoscere le procedure standard per la prevenzione di incidenti. Utilizzare il numero di istruzione presente alla fine di ciascuna avvertenza per individuare le traduzioni delle avvertenze riportate in questo documento.

CONSERVARE QUESTE ISTRUZIONI

Advarsel **VIKTIGE SIKKERHETSINSTRUKSJONER**

Dette advarselssymbolet betyr fare. Du er i en situasjon som kan føre til skade på person. Før du begynner å arbeide med noe av utstyret, må du være oppmerksom på farene forbundet med elektriske kretser, og kjenne til standardprosedyrer for å forhindre ulykker. Bruk nummeret i slutten av hver advarsel for å finne oversettelsen i de oversatte sikkerhetsadvarslene som fulgte med denne enheten.

TA VARE PÅ DISSE INSTRUKSJONENE

Aviso **INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

Este símbolo de aviso significa perigo. Você está em uma situação que poderá ser causadora de lesões corporais. Antes de iniciar a utilização de qualquer equipamento, tenha conhecimento dos perigos envolvidos no manuseio de circuitos elétricos e familiarize-se com as práticas habituais de prevenção de acidentes. Utilize o número da instrução fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham este dispositivo.

GUARDE ESTAS INSTRUÇÕES

¡Advertencia! **INSTRUCCIONES IMPORTANTES DE SEGURIDAD**

Este símbolo de aviso indica peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considere los riesgos de la corriente eléctrica y familiarícese con los procedimientos estándar de prevención de accidentes. Al final de cada advertencia encontrará el número que le ayudará a encontrar el texto traducido en el apartado de traducciones que acompaña a este dispositivo.

GUARDE ESTAS INSTRUCCIONES

Varning! **VIKTIGA SÄKERHETSANVISNINGAR**

Denna varningssignal signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanliga förfaranden för att förebygga olyckor. Använd det nummer som finns i slutet av varje varning för att hitta dess översättning i de översatta säkerhetsvarningar som medföljer denna anordning.

SPARA DESSA ANVISNINGAR

Figyelem **FONTOS BIZTONSÁGI ELOÍRÁSOK**

Ez a figyelmezeto jel veszélyre utal. Sérülésveszélyt rejto helyzetben van. Mielott bármely berendezésen munkát végezte, legyen figyelemmel az elektromos áramkörök okozta kockázatokra, és ismerkedjen meg a szokásos balesetvédelmi eljárásokkal. A kiadványban szereplo figyelmeztetések fordítása a készülékhez mellékelt biztonsági figyelmeztetések között található; a fordítás az egyes figyelmeztetések végén látható szám alapján keresheto meg.

ORIZZE MEG EZEKET AZ UTASÍTÁSOKAT!

Предупреждение **ВАЖНЫЕ ИНСТРУКЦИИ ПО СОБЛЮДЕНИЮ ТЕХНИКИ БЕЗОПАСНОСТИ**

Этот символ предупреждения обозначает опасность. То есть имеет место ситуация, в которой следует опасаться телесных повреждений. Перед эксплуатацией оборудования выясните, каким опасностям может подвергаться пользователь при использовании электрических цепей, и ознакомьтесь с правилами техники безопасности для предотвращения возможных несчастных случаев. Воспользуйтесь номером заявления, приведенным в конце каждого предупреждения, чтобы найти его переведенный вариант в переводе предупреждений по безопасности, прилагаемом к данному устройству.

СОХРАНИТЕ ЭТИ ИНСТРУКЦИИ

警告　重要的安全性说明

此警告符号代表危险。您正处于可能受到严重伤害的工作环境中。在您使用设备开始工作之前，必须充分意识到触电的危险，并熟练掌握防止事故发生的标准工作程序。请根据每项警告结尾提供的声明号码来找到此设备的安全性警告说明的翻译文本。

请保存这些安全性说明

警告　安全上の重要な注意事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。警告の各国語版は、各注意事項の番号を基に、装置に付属の「Translated Safety Warnings」を参照してください。

これらの注意事項を保管しておいてください。

주의　중요 안전 지침

이 경고 기호는 위험을 나타냅니다. 작업자가 신체 부상을 일으킬 수 있는 위험한 환경에 있습니다. 장비에 작업을 수행하기 전에 전기 회로와 관련된 위험을 숙지하고 표준 작업 관례를 숙지하여 사고를 방지하십시오. 각 경고의 마지막 부분에 있는 경고문 번호를 참조하여 이 장치와 함께 제공되는 번역된 안전 경고문에서 해당 번역문을 찾으십시오.

이 지시 사항을 보관하십시오.

Aviso　INSTRUÇÕES IMPORTANTES DE SEGURANÇA

Este símbolo de aviso significa perigo. Você se encontra em uma situação em que há risco de lesões corporais. Antes de trabalhar com qualquer equipamento, esteja ciente dos riscos que envolvem os circuitos elétricos e familiarize-se com as práticas padrão de prevenção de acidentes. Use o número da declaração fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham o dispositivo.

GUARDE ESTAS INSTRUÇÕES

Advarsel　VIGTIGE SIKKERHEDSANVISNINGER

Dette advarselssymbol betyder fare. Du befinder dig i en situation med risiko for legemesbeskadigelse. Før du begynder arbejde på udstyr, skal du være opmærksom på de involverede risici, der er ved elektriske kredsløb, og du skal sætte dig ind i standardprocedurer til undgåelse af ulykker. Brug erklæringsnummeret efter hver advarsel for at finde oversættelsen i de oversatte advarsler, der fulgte med denne enhed.

GEM DISSE ANVISNINGER

تحذير　إرشادات الأمان الهامة

يوضح رمز التحذير هذا وجود خطر. وهذا يعني أنك متواجد في مكان قد ينتج عنه التعرض لإصابات. قبل بدء العمل، احذر مخاطر التعرض للصدمات الكهربائية وكن على علم بالإجراءات القياسية للحيلولة دون وقوع أي حوادث. استخدم رقم البيان الموجود في أخر كل تحذير لتحديد مكان ترجمته داخل تحذيرات الأمان المترجمة التي تأتي مع الجهاز.
قم بحفظ هذه الإرشادات

Upozorenje

VAŽNE SIGURNOSNE NAPOMENE

Ovaj simbol upozorenja predstavlja opasnost. Nalazite se u situaciji koja može prouzročiti tjelesne ozljede. Prije rada s bilo kojim uređajem, morate razumjeti opasnosti vezane uz električne sklopove, te biti upoznati sa standardnim načinima izbjegavanja nesreća. U prevedenim sigurnosnim upozorenjima, priloženima uz uređaj, možete prema broju koji se nalazi uz pojedino upozorenje pronaći i njegov prijevod.

SAČUVAJTE OVE UPUTE

Upozornění

DŮLEŽITÉ BEZPEČNOSTNÍ POKYNY

Tento upozorňující symbol označuje nebezpečí. Jste v situaci, která by mohla způsobit nebezpečí úrazu. Před prací na jakémkoliv vybavení si uvědomte nebezpečí související s elektrickými obvody a seznamte se se standardními opatřeními pro předcházení úrazům. Podle čísla na konci každého upozornění vyhledejte jeho překlad v přeložených bezpečnostních upozorněních, která jsou přiložena k zařízení.

USCHOVEJTE TYTO POKYNY

Προειδοποίηση

ΣΗΜΑΝΤΙΚΕΣ ΟΔΗΓΙΕΣ ΑΣΦΑΛΕΙΑΣ

Αυτό το προειδοποιητικό σύμβολο σημαίνει κίνδυνο. Βρίσκεστε σε κατάσταση που μπορεί να προκαλέσει τραυματισμό. Πριν εργαστείτε σε οποιοδήποτε εξοπλισμό, να έχετε υπόψη σας τους κινδύνους που σχετίζονται με τα ηλεκτρικά κυκλώματα και να έχετε εξοικειωθεί με τις συνήθεις πρακτικές για την αποφυγή ατυχημάτων. Χρησιμοποιήστε τον αριθμό δήλωσης που παρέχεται στο τέλος κάθε προειδοποίησης, για να εντοπίσετε τη μετάφρασή της στις μεταφρασμένες προειδοποιήσεις ασφαλείας που συνοδεύουν τη συσκευή.

ΦΥΛΑΞΤΕ ΑΥΤΕΣ ΤΙΣ ΟΔΗΓΙΕΣ

אזהרה

הוראות בטיחות חשובות

סימן אזהרה זה מסמל סכנה. אתה נמצא במצב העלול לגרום לפציעה. לפני שתעבוד עם ציוד כלשהו, עליך להיות מודע לסכנות הכרוכות במעגלים חשמליים ולהכיר את הנהלים המקובלים למניעת תאונות. השתמש במספר ההוראה המסופק בסופה של כל אזהרה כד לאתר את התרגום באזהרות הבטיחות המתורגמות שמצורפות להתקן.

שמור הוראות אלה

Opomena

ВАЖНИ БЕЗБЕДНОСНИ НАПАТСТВИЈА

Симболот за предупредување значи опасност. Се наоѓате во ситуација што може да предизвика телесни повреди. Пред да работите со опремата, бидете свесни за ризикот што постои кај електричните кола и треба да ги познавате стандардните постапки за спречување на несреќни случаи. Искористете го бројот на изјавата што се наоѓа на крајот на секое предупредување за да го најдете неговиот период во преведените безбедносни предупредувања што се испорачани со уредот.

ЧУВАЈТЕ ГИ ОВИЕ НАПАТСТВИЈА

Ostrzeżenie

WAŻNE INSTRUKCJE DOTYCZĄCE BEZPIECZEŃSTWA

Ten symbol ostrzeżenia oznacza niebezpieczeństwo. Zachodzi sytuacja, która może powodować obrażenia ciała. Przed przystąpieniem do prac przy urządzeniach należy zapoznać się z zagrożeniami związanymi z układami elektrycznymi oraz ze standardowymi środkami zapobiegania wypadkom. Na końcu każdego ostrzeżenia podano numer, na podstawie którego można odszukać tłumaczenie tego ostrzeżenia w dołączonym do urządzenia dokumencie z tłumaczeniami ostrzeżeń.

NINIEJSZE INSTRUKCJE NALEŻY ZACHOWAĆ

Upozornenie

DÔLEŽITÉ BEZPEČNOSTNÉ POKYNY

Tento varovný symbol označuje nebezpečenstvo. Nachádzate sa v situácii s nebezpečenstvom úrazu. Pred prácou na akomkoľvek vybavení si uvedomte nebezpečenstvo súvisiace s elektrickými obvodmi a oboznámte sa so štandardnými opatreniami na predchádzanie úrazom. Podľa čísla na konci každého upozornenia vyhľadajte jeho preklad v preložených bezpečnostných upozorneniach, ktoré sú priložené k zariadeniu.

USCHOVAJTE SI TENTO NÁVOD

Related Publications

You can order printed copies of documents with a DOC-xxxxxx= number. For more information, see the "Obtaining Documentation" section on page xiv.

These documents provide complete information about the switch and are available from this Cisco.com site:

http://www.cisco.com/en/US/products/ps6748/tsd_products_support_series_home.html

- *Cisco Catalyst Blade Switch 3030 Getting Started Guide* (order number DOC-7817052=)
- *Regulatory Compliance and Safety Information for the Cisco Catalyst Blade Switch 3030* (order number DOC-7817053=)
- *Release Notes for the Cisco Catalyst Blade Switch 3030, Cisco IOS Release 12.2(25)SEE* (not orderable but available on Cisco.com)

Note Before installing, configuring, or upgrading the switch, see the release notes on Cisco.com for the latest information.

- *Cisco Catalyst Blade Switch 3030 Software Configuration Guide* (order number DOC-7817261=)
- *Cisco Catalyst Blade Switch 3030 Command Reference* (order number DOC-7817262=)
- *Cisco Catalyst Blade Switch 3030 System Message Guide* (order number DOC-7817263=)
- *Cisco Gigabit Ethernet Transceiver Modules Compatibility Matrix* (not orderable but available on Cisco.com)

- *Cisco 100-Megabit Ethernet SFP Modules Compatibility Matrix* (not orderable but available on Cisco.com)
- *Cisco Small Form-Factor Pluggable Modules Compatibility Matrix* (not orderable but available on Cisco.com)
- *Compatibility Matrix for 1000BASE-T Small Form-Factor Pluggable Modules* (not orderable but available on Cisco.com)

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Product Overview

This chapter provides a functional overview of the Cisco Catalyst Blade Switch 3030, also referred to as the *switch module* or *switch*. The switch module is a 16-port Ethernet switch that can be installed in the Dell Modular Server Chassis to aggregate network traffic from the internal server blades. The Dell Modular Server Chassis—also referred to as the *server chassis*—is a system that supports up to ten server modules and up to four Ethernet switch modules. The switch module is installed in one of the chassis I/O module bays on the rear panel of the server chassis.

You can connect the uplink ports to other devices such as switches, routers, Cisco Wireless Access Point workstations, Cisco IP phones, or other networking equipment. You can also connect standalone servers or PCs to those ports.

These topics are included:

- Features, page 1-1
- Front Panel Description, page 1-2
- Rear Panel Description, page 1-5
- Management Options, page 1-6

Features

The 16-port Gigabit Ethernet switch can be deployed as a backbone switch, aggregating 10BASE-T, 100BASE-TX, and 1000BASE-T Ethernet traffic from other network devices. Refer to the switch software configuration guide for examples showing how you might deploy the switch in your network.

These are the switch features:

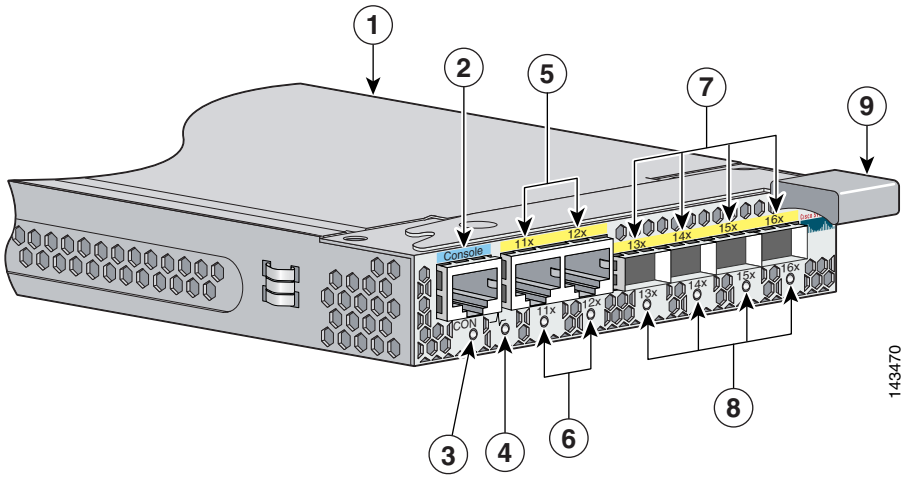
- 10 internal Gigabit Ethernet 1000BASE-X ports
- 1 console port
- 2 external 10/100/1000BASE-T copper Gigabit Ethernet ports
- 4 external small-form factor pluggable (SFP) module uplink ports that support 1000BASE-SX fiber optic and 10/100/1000BASE-T copper (only Cisco SFP modules are supported)

Note When installed in the switch, 1000BASE-T SFP modules can operate at 10, 100, or 1000 Mbps in full-duplex mode or at 10 or 100 Mbps in half-duplex mode.

Front Panel Description

Ten of the ports on the 16-port Gigabit Ethernet switch are internal 1000BASE-X ports that connect to the server chassis through the backplane. Figure 1-1 shows the console port, the two external 10/100/1000BASE-T copper ports, and the four external SFP module uplink ports that support 1000BASE-SX and 10/100/1000BASE-T copper. Only Cisco SFP modules are supported on the switch.

Figure 1-1 The Cisco Gigabit Ethernet Switch Module



1	Switch module	**6**	Gigabit Ethernet port LEDs
2	Console port	**7**	SFP module ports
3	Console port LED	**8**	SFP module port LEDs
4	System Status/ID LED	**9**	Release latch
5	External Gigabit Ethernet ports		

Each port has an LED associated with it. The Dell Remote Access Controller/Modular Chassis (DRAC/MC) management board controls the System Status/ID LED.

Switch Console Port

You can connect the switch to a PC by means of the console port and an RJ-45-to-DB-9 female cable. If you want to connect the switch console port to a terminal, you need to provide an RJ-45-to-DB-25 female DTE adapter. You can order a kit (part number ACS-DSBUASYN=) containing that adapter from Cisco. For console port and adapter pinout information, see the "Connector and Cable Specifications" section on page B-1.

For information on the server chassis DRAC/MC console port, see the server chassis documentation.

10/100/1000 Ports

The two copper Ethernet ports operate at 10, 100, or 1000 Mbps and support autonegotiation and full-duplex operation. When set for autonegotiation, the port senses the speed and duplex settings of the attached device and advertises its own capabilities. If the connected device also supports autonegotiation, the switch port negotiates the best connection (that is, the fastest line speed that both devices support and full-duplex transmission if the attached device supports it) and configures itself accordingly. In all cases, the attached device must be within 328 feet (100 meters).

You can disable autonegotiation for the two 10/100/1000BASE-T ports by using the Cisco IOS command-line interface (CLI). For more information, see the command reference and the software configuration guide for the switch.

The ten internal downlink ports are 1000BASE-X with no negotiation for speed.

Note 1000BASE-T traffic requires at least a Category 5 cable. 10BASE-T traffic can use Category 3 or Category 4 cables.

When connecting the switch to workstations, servers, routers, and Cisco IP Phones, be sure that the cable is a straight-through cable. When you connect the switch to switches or hubs, use a crossover cable. When you use a straight-through or crossover cable for 1000BASE-T connections, be sure to use a twisted four-pair, Category 5 cable for proper operation. Pinouts for the cables are described in Appendix B, “Connector and Cable Specifications.”

Note You can use the **mdix auto** interface configuration command in the CLI to enable the automatic medium-dependent interface crossover (auto-MDIX) feature. When the auto-MDIX feature is enabled, the switch detects the required cable type for copper Ethernet connections and configures the interfaces accordingly. Therefore, you can use either a crossover or a straight-through cable for connections to a copper 10/100/1000 or 1000BASE-T SFP module port on the switch, regardless of the type of device on the other end of the connection.

The auto-MDIX feature is enabled by default. For configuration information for this feature, refer to the switch software configuration guide or the switch command reference.

SFP Module Slots

The switch uses Gigabit Ethernet SFP modules to establish fiber-optic connections. These transceiver modules are field-replaceable, providing the uplink interfaces when inserted in an SFP module slot. You can use the SFP modules for Gigabit uplink connections to other switches. You use fiber-optic cables with LC or MT-RJ connectors to connect to a fiber-optic SFP module. You use Category 5 cable with RJ-45 connectors to connect to a copper SFP module.

The four external SFP module ports operate at 1000 Mbps when fiber-optic SFP modules are installed and operate at 10/100/1000 Mbps when copper SFP modules are installed. Autonegotation is supported on copper SPF modules, but not on fiber-optic SFP modules.

See the release notes for the latest information about which SFP module types are supported.

For more information about the SFP modules, refer to your SFP module documentation.

LEDs

The switch has eight LEDs including an LED for each external port, one LED for the console port, and one LED used by server chassis management board (see Figure 1-1). You can use the switch LEDs to monitor switch activity and performance. Graphical representations of the LEDs described in this section are visible in the device manager.

System Status/ID LED

The System Status/ID LED is controlled by the server DRAC/MC and shows whether the system is receiving power and functioning properly. Table 1-1 lists the LED colors and their meanings.

Table 1-1 System LED

Color	System Status
Off	System is operating normally.
Blinking green	System is receiving power but is not functioning properly. Log into the DRAC/MC to get more details about the failure mode.

The chassis controls its own cooling and temperature. The DRAC/MC temperature sensor monitors the temperature of any modules that are installed in the chassis. The DRAC/MC also controls the chassis fan speed. The switch does not have its own fan.

Console Port LEDs

The console port LED is either green or amber and displays information about the console port. Table 1-3 describes the console port LED colors and their meanings.

Table 1-2 Meaning of Console Port LED Colors

LED Color	Meaning
Off	The bootloader is initializing.
Solid green	The switch module console port is active.
Solid amber	The switch module console port is inactive; the backplane console is active.
Solid green or amber	Cisco IOS is operating normally.

Port LEDs

The port LEDs display information about each individual port. The port LEDs are green and/or amber. Table 1-3 describes the port LED colors and their meanings.

Table 1-3 Meaning of Port LED Colors

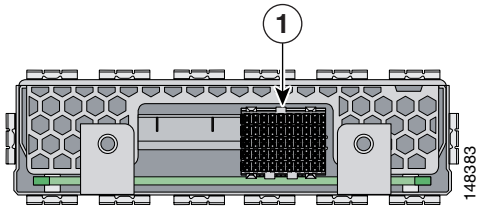
LED Color	Meaning
Off	No link established
Solid green	Link established but no activity
Blinking green	Traffic on an established link
Solid amber	Port disabled, either error or STP[1] disabled
Alternating green and amber	Link fault

1. STP = Spanning Tree Protocol

Rear Panel Description

The switch module connects to the server chassis through the backplane connector on the switch rear panel. See Figure 1-2.

Figure 1-2 Switch Rear Panel



1	Backplane connector

Note You must engage the release latch to secure the connection to the backplane. See Figure 1-1.

Power Connectors

The DRAC/MC controls power to the switch module. After the DRAC/MC detects the presence of the switch module, it moves the switch module to the full power state. The switch software is not involved in power control functions.

Management Options

This section describes management options for the switch module:

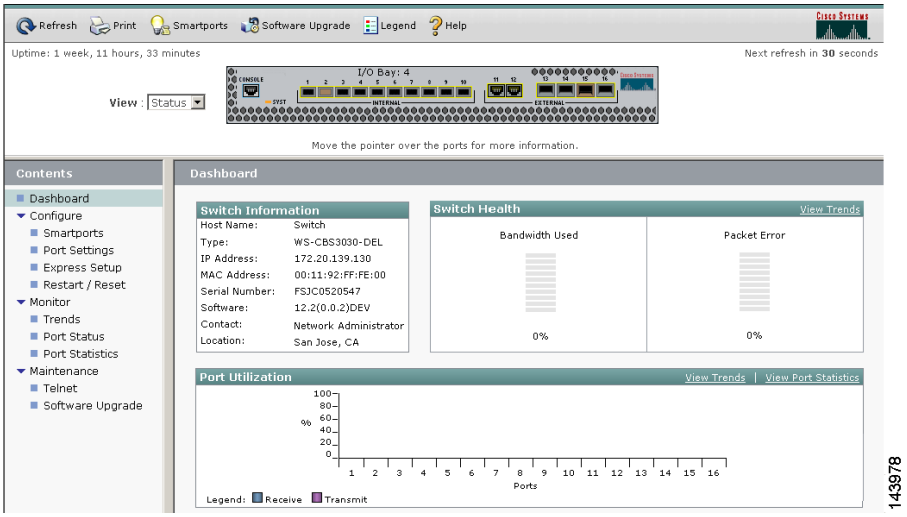
- Using the Device Manager, page 1-6
- Using the Command-Line Interface, page 1-7
- Using SNMP, page 1-7

Using the Device Manager

The simplest way to manage the switch is by using the device manager that is in the switch memory. This is an easy-to-use web interface that offers quick configuration and monitoring. You can access the device manager through a web browser from anywhere in your network.

The device manager dashboard is shown in Figure 1-3.

Figure 1-3 Device Manager Dashboard



Follow these steps to access the device manager:

1. Launch a web browser on your PC or workstation.
2. Enter the switch IP address in the web browser, and press **Enter**. The device manager page appears.
3. Use the device manager to perform basic switch configuration and monitoring. Refer to the device manager online help for more information.

Using the Command-Line Interface

The switch CLI) is based on Cisco IOS software and enhanced to support desktop-switching features. You can fully configure and monitor the switch from the CLI. You can access the CLI either by connecting your management station directly to the switch console port or by using Telnet from a remote management station. Refer to the switch module command reference on Cisco.com for more information.

For quick setup instructions that use the CLI, go to Appendix C, "Configuring the Switch with the CLI-Based Setup Program."

Using SNMP

You can use SNMP management applications such as CiscoWorks. You also can manage the switch from an SNMP-compatible workstation that is running platforms such as SunNet Manager.

Network Configurations

Refer to the switch software configuration guide on Cisco.com for an explanation of network configuration concepts. The software configuration guide also provides examples of network configurations that use the switch to create dedicated network segments that are interconnected through Gigabit Ethernet connections.

Switch Installation

This chapter provides instructions on how to install your Cisco Catalyst Blade Switch 3030—also referred to as the *switch module*—in the Dell Modular Server Chassis and how to set up and configure your switch module. The Dell Modular Server Chassis—also referred to as the *server chassis*—is a system that supports up to ten server modules and up to four Ethernet switch modules. The switch module is installed in one of the chassis I/O module bays on the rear panel of the server chassis.

This chapter also describes how to interpret the power-on self-test (POST) that ensures proper operation and how to make connections to the switch.

Read the topics and perform the procedures in this order:

- Preparing for Installation, page 2-1
- Dell Modular Server Chassis Architecture, page 2-5
- Installing the Switch Module into the Server Chassis, page 2-6
- Installing and Removing SFP Modules, page 2-13
- Connecting to the 10/100/1000 Ports, page 2-16
- Connecting to SFP Modules, page 2-17
- Where to Go Next, page 2-19

Preparing for Installation

This section covers these topics:

- Warnings, page 2-1
- Installation Guidelines, page 2-3
- Verifying Package Contents, page 2-4

Warnings

These warnings are translated into several languages in the *Regulatory Compliance and Safety Information for the Cisco Catalyst Blade Switch 3030* that ships with the product. The EMC regulatory statements are also included in that guide.

Warning **To prevent the switch from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of 113°F (45°C). To prevent airflow restriction, allow at least 3 inches (7.6 cm) of clearance around the ventilation openings.** Statement 17B

Warning **Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.** Statement 43

Warning **Ethernet cables must be shielded when used in a central office environment.** Statement 171

Warning **Do not work on the system or connect or disconnect cables during periods of lightning activity.** Statement 1001

Warning **Read the installation instructions before connecting the system to the power source.** Statement 1004

Warning **Class 1 laser product.** Statement 1008

Warning **This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security.** Statement 1017

Warning **This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.** Statement 1024

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030

Warning **Ultimate disposal of this product should be handled according to all national laws and regulations.** Statement 1040

Warning **For connections outside the building where the equipment is installed, the following ports must be connected through an approved network termination unit with integral circuit protection. 10/100/1000 Ethernet** Statement 1044

Warning **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.** Statement 1051

Warning **Installation of the equipment must comply with local and national electrical codes.** Statement 1074

Installation Guidelines

Before you install the switch module in the server chassis, read these guidelines:

- Review and become familiar with the safety and handling guidelines specified in the server chassis *Product Information Guide*.
- Review the "Warnings" section on page 2-1 and the *Regulatory Compliance and Safety Information for the Cisco Catalyst Blade Switch 3030* that accompanies this guide.
- To help ensure proper cooling and system reliability, keep these points in mind:
  - Each server chassis I/O module bay must contain either a module or an end-cap (blank plug).
  - When you remove a hot-swap module, you must replace it with an identical module or an end-cap (blank plug) within 1 minute of removal.

Caution To prevent electrostatic-discharge (ESD) damage when installing switch modules, follow your normal board and component handling procedures.

Note When you install a switch module, you do not need to power down the server modules or the chassis.

Note The initial configuration assumes that the switch module was never configured, that it is in the same state as when it was received, and that it is not configured with a default username and password.

Be sure to observe these requirements:

- For copper Ethernet ports, including 10/100/1000 ports and 1000BASE-T SFP module ports, cable lengths from the switch to connected devices can be up to 328 feet (100 meters).
- See the documentation for the SFP module for more information about cable specifications for 1for the SFP module connections. Each port must match the wave-length specifications on the other end of the cable, and the cable must not exceed the stipulated cable length for reliable communications.

Note When using shorter lengths of single-mode fiber-optic cable, you might need to insert an inline optical attenuator in the link to avoid overloading the receiver.

- Operating environment is within the ranges listed in Appendix A, "Technical Specifications."
- Cabling is away from sources of electrical noise, such as radios, power lines, and fluorescent lighting fixtures. Make sure the cabling is safely away from other devices that might damage the cables.
- Airflow around the switch and through the vents is unrestricted.
- Temperature around the unit does not exceed 113°F (45°C).

Verifying Package Contents

Note Carefully remove the contents from the shipping container, and check each item for damage. If any item is missing or damaged, contact your Cisco representative or reseller for support. Return all packing material to the shipping container, and save it.

These items ship with your switch module:

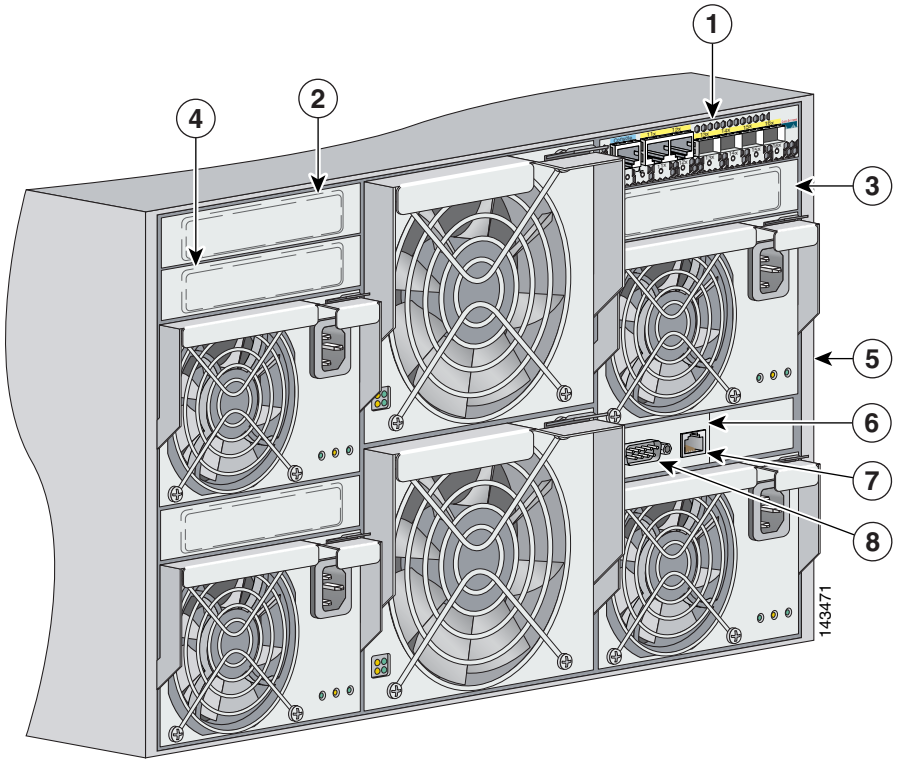
- Console cable
- *Cisco Catalyst Blade Switch 3030 Getting Started Guide*
- *Regulatory Compliance and Safety Information for the Cisco Catalyst Blade Switch 3030*
- Registration card

Note If the switch modules are ordered with the server chassis, the switch modules are already installed, and no unpacking is required. The unpacking procedure applies only if a switch module is ordered separately.

Dell Modular Server Chassis Architecture

The four chassis I/O module bays are on the rear panel (see Figure 2-1). You can insert switch modules into the chassis I/O module bays 1 and 2. Use bays 3 and 4 for switch modules only if a Gigabit Ethernet daughter card is installed on the server modules.

Figure 2-1 Dell Modular Server Chassis



1	Bay 1 (populated with switch module)	**5**	Rear panel of server chassis
2	Bay 2	**6**	DRAC/MC[1] management board
3	Bay 3	**7**	Ethernet port
4	Bay 4	**8**	RS-232 port

1. DRAC/MC: Dell Remote Access Controller/Modular Chassis management board

Consider these prerequisites before installing your switch module:

- Bay 1 and bay 2 are a pair. Bay 1 must be populated before bay 2. If bay 2 is used, the I/O module in bay 2 must be the same type as the one in bay 1.
- Bay 3 and bay 4 are a pair. Bay 3 must be populated before bay 4. If bay 4 is used, the I/O module in bay 4 must be the same type as the one in bay 3.

For more information about the components of the information panel, see the *Dell PowerEdge 1855 Systems User's Guide* and the *Dell PowerEdge 1855 Systems Installation and Troubleshooting Guide*.

Installing the Switch Module into the Server Chassis

For a description of the switch module, see the "Features" section on page 1-1.

Follow these steps to install the switch module into the server chassis:

Step 1 Obtain and make note of this information from your network administrator before you begin the switch module installation:

- Switch IP address
- Subnet mask (IP netmask)
- Default gateway (router)
- Enable secret password (encrypted)
- Enable password (not encrypted)
- Telnet password
- SNMP community strings (optional)

Step 2 Select a chassis I/O module bay in which to install the switch module. Follow the prerequisites listed in the "Dell Modular Server Chassis Architecture" section on page 2-5.

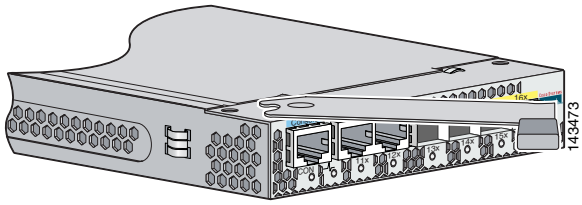
Step 3 Remove the end-cap (blank plug) from the selected bay. Store the end-cap (blank plug) for future use.

Step 4 If you have not already done so, touch the static-protective package that contains the switch module to an unpainted metal part of the server chassis for at least 2 seconds.

Step 5 Remove the switch module from its static-protective package.

Step 6 Ensure that the release latch on the switch module is in the open position (perpendicular to the module). (See Figure 2-2.)

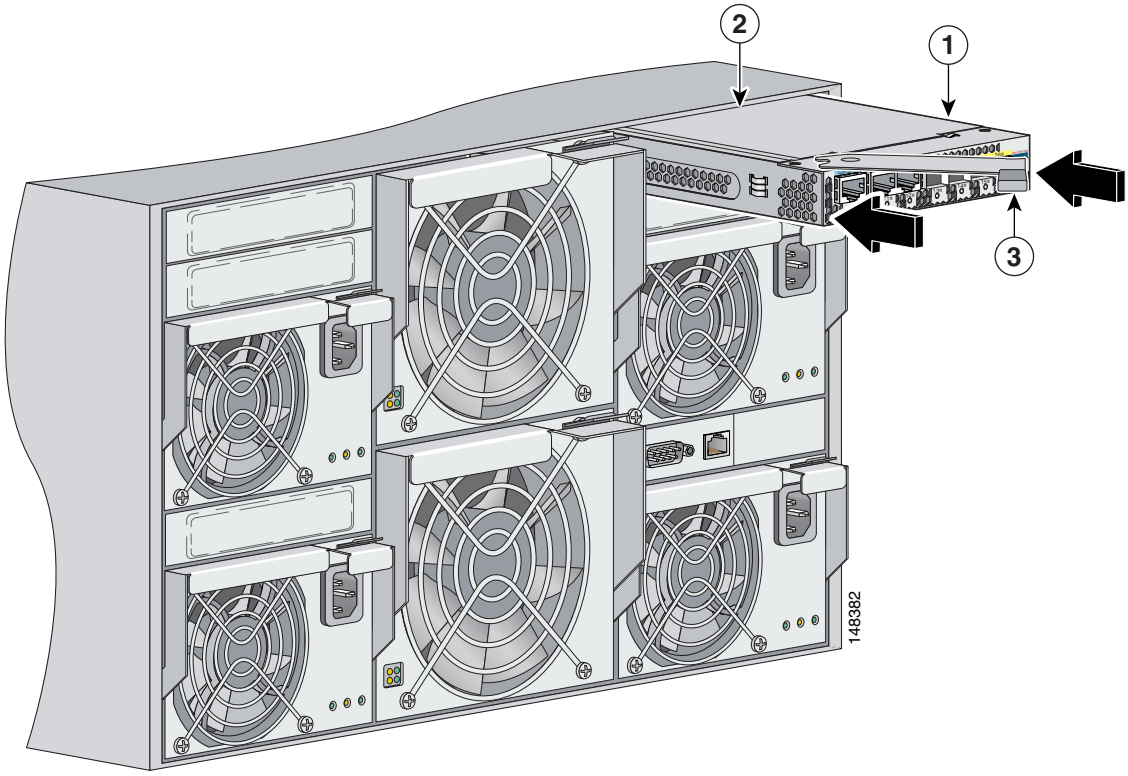
Figure 2-2 Switch Module Release Latch in the Open Position



Step 7 Slide the switch module into the appropriate bay until it stops.

Step 8 Push the release latch on the front of the switch module to the closed position. Figure 2-3 shows the switch module being inserted into the server chassis.

Figure 2-3 Inserting the Switch Module into the Server Chassis



1	Switch module	**3**	Release latch
2	Server chassis		

Configuring the Switch Module

Follow one of these procedures:

- To run the terminal emulation program through the switch module console port, go to "Connecting through the Switch Module Console Port" section on page 2-8.
- To run the terminal emulation program through the DRAC/MC port, go to "Connecting through the DRAC/MC" section on page 2-9.

Connecting through the Switch Module Console Port

This section describes how to connect a PC through the switch module console port to set up the switch.

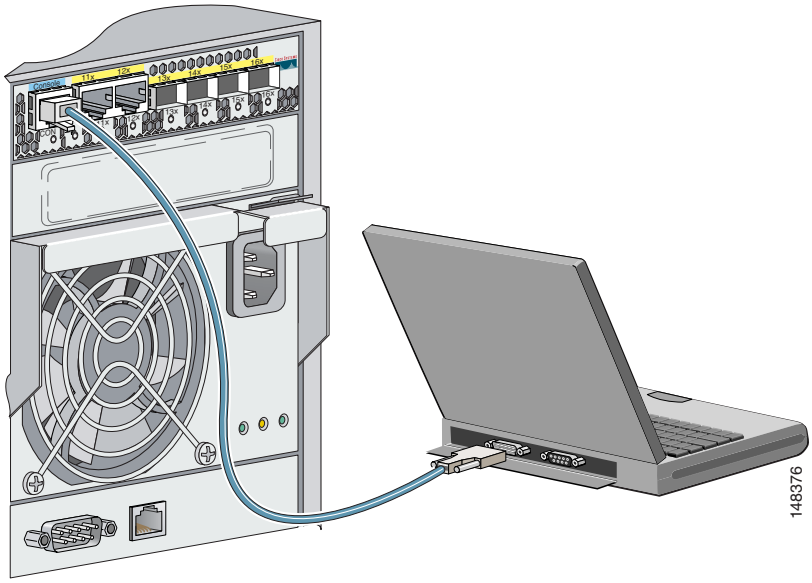
Note To run the system configuration dialog, you must first connect the switch to a PC to run a terminal emulation program. There are two ways you can connect the PC to the switch: either through the switch console port or through the DRAC/MC console port. Instructions for these two procedures are included in this section.

If you connect to the switch through the DRAC/MC, the switch console port is disabled. After you have completed the configuration procedure, you must use the **disconnect** command to close the active console port and to re-enable the switch console port. Enter **logout** to log out of the switch. Finally, enter a tilde (~) and then a period (dot) to disconnect the DRAC/MC from the switch.

Follow these steps when connecting through the switch module console port:

Step 1 Connect one end of the console cable to the switch module console port. Connect the other end of the cable to the serial port of the computer that is running the terminal emulation application. (See Figure 2-4.)

Figure 2-4 Connecting through the Switch Module Console Cable



Step 2 Start the terminal emulation session so that you can see the output display from the power-on self-test (POST). The terminal-emulation software—a PC application such as Hyperterminal or ProcommPlus—makes communication between the switch and your PC or terminal possible.

Step 3 Configure the baud rate and character format of the PC or terminal to match these console port default characteristics:

- 9600 baud
- 8 data bits
- 1 stop bit
- No parity
- None (flow control)

Step 4 Go to the "Waiting for POST to Complete" section on page 2-11 to finish configuring the switch module.

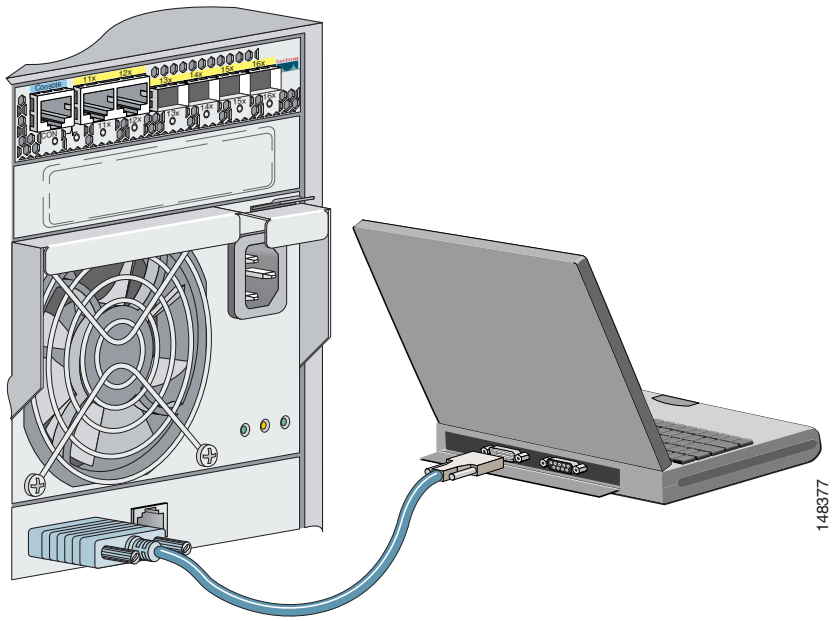
Connecting through the DRAC/MC

Follow these steps when connecting through the DRAC/MC:

Step 1 Connect one end of a DB9 null-modem or crossover cable to the RS-232 console serial port of the DRAC/MC. Connect the other end of the cable to the RS-232 console serial port of the computer. (See Figure 2-5.)

Note The default data rate of the DRAC/MC console serial port is 115200 baud.

Figure 2-5 Connecting through the DRAC/MC Serial Port



Step 2 On the PC terminal emulation program:

a. Set the data format to 8 data bits, 1 stop bit, and no parity.

b. Set the terminal emulation speed to 115200 baud.

c. Set **Flow Control** to none.

d. Under **Properties**, select **VT100** for Emulation mode.

e. Select Terminal keys for Function, Arrow, and Ctrl keys. Ensure that the setting is for Terminal keys (not Windows keys).

Note When using HyperTerminal with Microsoft Windows 2000, ensure that you have Windows 2000 Service Pack 2 or later installed. With Windows 2000 Service Pack 2, the arrow keys function properly in the HyperTerminal VT100 emulation. Go to www.microsoft.com for information on Windows 2000 service packs.

Step 3 On the console monitor, the DRAC/MC application displays a login screen. Log in by using these defaults:

username **root**
password **calvin**

The DRAC/MC command-line interface (CLI) prompt **DRAC/MC:** appears.

Step 4 If the server chassis is off, use this command to power it on:

```
racadm chassisaction -m chassis powerup
```

The switch module inserted into the chassis I/O bay automatically powers on when the server chassis powers on. For more information on configuring the server chassis by using the CLI see the *Dell Remote Access Controller/Modular Chassis User's Guide*.

Step 5 Power cycle the switch module by using this command on the DRAC/MC console application:

```
racadm chassisaction -m switch-N powercycle
```

where *N* is the chassis I/O module bay number in which the switch module is inserted.

Step 6 Redirect the DRAC/MC console to the switch module internal serial console interface. Enter this command at the DRAC/MC command prompt:

```
connect switch-N
```

where *N* is the chassis I/O module bay number in which the switch module is inserted.

To return to the command prompt, press this key sequence:
Enter ~.

First press **Enter**, press tilde **~** (remember to press the <Shift> key if the tilde character is located in the upper register of your keyboard), and then press period **.** (dot).

Step 7 Go to the "Waiting for POST to Complete" section on page 2-11 to finish configuring the switch module.

Waiting for POST to Complete

Follow these steps:

Step 1 Wait for the switch to complete POST. It might take several minutes for the switch to complete POST.

Step 2 Verify that POST has completed by confirming that the System Status/ID LED is off and that the Console LED is solid green or amber. If the switch fails POST because of a misconfiguration or error, the System Status/ID LED blinks green, and the Console LED is off.

Log into the DRAC/MC console to get more details about the failure mode.

POST errors are usually fatal. Call Cisco Customer Support immediately if your switch fails POST.

See item 4 in Figure 1-1 on page 1-2 for the location of the System Status/ID LED and the Console LED.

Step 3 Wait for the switch to complete flash initialization. When you see the prompt *Press Return to Get Started!*, press **Return** or **Enter**.

Step 4 Make sure that the System Status/ID LED on the switch module is off and that the Console LED is green or amber. This means that the switch module is operating properly.

Step 5 See the "Completing the Initial Configuration" section on page 2-11 for instructions on setting up and initially configuring the switch module.

Completing the Initial Configuration

Follow these steps to complete the setup program and to create an initial configuration for the switch.

Note For information about automatically configuring the switch, see the "Assigning the Switch IP Address and Default Gateway" chapter in the switch configuration guide.

Step 1 After you have pressed **Enter** or **Return** after the prompt to start the initial configuration setup program, enter **yes** at these prompts:

```
Would you like to terminate autoinstall? [yes]: yes

--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: yes

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:
```

Step 2 Enter a hostname for the switch after the prompt, and press **Return**.

The hostname is limited to 20 characters. Do not use *-n*, where n is a number, as the last character in a host name for any switch.

Step 3 Enter an enable secret password, and press **Return**.

The password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, allows spaces, but ignores leading spaces. The secret password is encrypted, and the enable password is in plain text.

Step 4 Enter an enable password, and press **Return**.

Step 5 Enter a virtual terminal (Telnet) password, and press **Return**.

The password can be from 1 to 25 alphanumeric characters, is case sensitive, allows spaces, but ignores leading spaces.

Step 6 (Optional) Configure Simple Network Management Protocol (SNMP) by responding to the prompts.

1. To configure SNMP later, press **Return** (which applies the default of no). If you accept the default, you can configure SNMP later through the CLI.

```
Configure SNMP Network Management? [no]:
```

2. To configure SNMP now, enter **yes**.

```
Configure SNMP Network Management? [no]: yes
Community string [public]: public
```

Step 7 Enter the interface name (physical interface or VLAN name) of the interface that connects to the management network, and press **Return**.

Enter **vlan1** for the interface name at this prompt.

Step 8 To configure the interface, enter **Yes** after the prompt, and then enter the switch IP address and subnet mask. Press **Return**.

The IP address and subnet mask shown here are examples:

```
Configuring interface Vlan1:
Configure IP on this interface? [yes]:
IP address for this interface [10.0.0.1]:
Subnet mask for this interface [255.255.255.0] : 255.255.255.0
Class A network is 10.0.0.1, 21 subnet bits; mask is /21
```

Step 9 Enter **no** when the prompt asks you if you would like to enable the switch as a cluster command switch. This switch will be a standalone switch.

```
Would you like to enable as a cluster command switch? [yes/no]: no
```

Note Clustering is not supported on the Cisco Catalyst Blade Switch 3030.

You have now completed the initial configuration of the switch, and the switch displays its initial configuration. An example of the output is shown here:

```
The following configuration command script was created:
hostname switch1
enable secret 5 $1$cagJ$e4LP91PNazfdADoNAZm6y0
enable password enable_password
line vty 0 15
password terminal-password
snmp-server community public
!
!
```

```
interface Vlan1
no shutdown
ip address 10.0.0.1 255.255.255.0
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2

. . . (output truncated)

interface GigabitEthernet0/16
!
end
```

Step 10 These choices appear:

```
[0] Go to the IOS command prompt without saving this config.

[1] Return back to the setup without saving this config.

[2] Save this configuration to nvram and exit.

If you want to save the configuration and use it the next time the switch reboots, save it
in NVRAM by selecting option 2.

Enter your selection [2]:2
```

Make your selection, and press **Return**.

Step 11 Disconnect the server chassis serial port or the switch console port from the PC. See the "Management Options" section on page 1-6 for information about managing the switch.

If you need to rerun the initial configuration dialog, see the "Configuring the Switch Module" section on page 2-7.

To use the CLI, enter commands at the *Switch*> prompt through the console port by using a terminal program or through the network by using Telnet. For configuration information, refer to the switch software configuration guide or the switch command reference.

Installing and Removing SFP Modules

These sections describe how to install and remove SFP modules. The modules are inserted into the SFP module slots on the front of the switch module. These field-replaceable modules provide uplink interfaces.

You can use any combination of SFP modules. Refer to the switch module release notes for the list of SFP modules that the switch supports. Each port must match the wave-length specifications on the other end of the cable, and the cable must not exceed the stipulated cable length for reliable communications. See the "Installation Guidelines" section on page 2-3 for cable stipulations for SFP connections.

Use only Cisco SFP modules on the switch. Each SFP module has an internal serial EEPROM that is encoded with security information. This encoding provides a way for Cisco to identify and validate that the SFP module meets the requirements for the switch.

For detailed instructions on installing, removing, and cabling the SFP module, refer to your SFP module documentation.

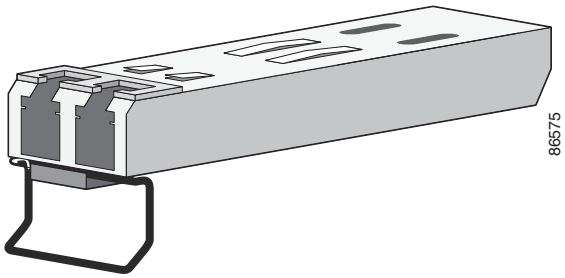
Installing SFP Modules into SFP Module Slots

Figure 2-6 shows an SFP module that has a bale-clasp latch.

Caution We strongly recommend that you do not install or remove fiber-optic SFP modules with cables attached because of the potential damage to the cables, the cable connector, or the optical interfaces in the SFP module. Disconnect all cables before removing or installing an SFP module.

Removing and installing an SFP module can shorten its useful life. Do not remove and insert SFP modules more often than is absolutely necessary.

Figure 2-6 SFP Module with a Bale-Clasp Latch



To insert an SFP module into the module slot, follow these steps:

Step 1 Attach an ESD-preventive wrist strap to your wrist and to a bare metal surface on the chassis.

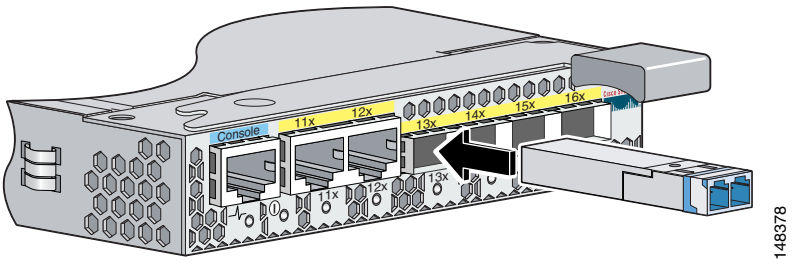
Step 2 Find the send (TX) and receive (RX) markings that identify the top side of the SFP module.

Note On some SFP modules, the send and receive (TX and RX) markings might be replaced by arrows that show the direction of the connection, either send or receive (TX or RX).

Step 3 Align the SFP module in front of the slot opening.

Step 4 Insert the SFP module into the slot until you feel the connector on the module snap into place in the rear of the slot. (See Figure 2-7.)

Figure 2-7 Installing an SFP Module into an SFP Module Slot



Removing SFP Modules from SFP Module Slots

To remove an SFP module from a module receptacle, follow these steps:

Step 1 Attach an ESD-preventive wrist strap to your wrist and to a bare metal surface on the chassis.

Step 2 Disconnect the cable from the SFP module.

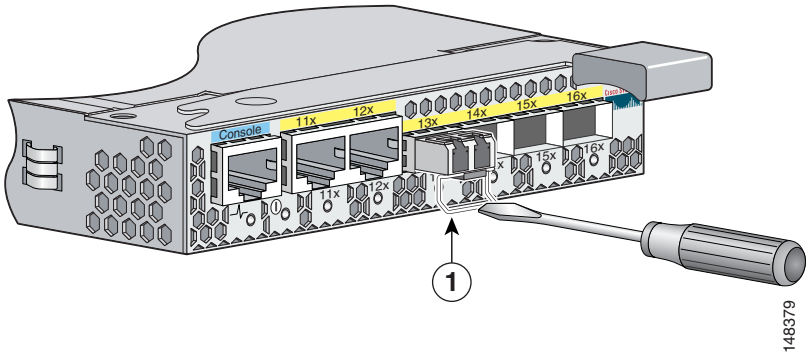
Tip For reattachment, note which cable connector plug is send (TX) and which is receive (RX).

Step 3 For fiber-optic SFP modules, insert a dust plug into the optical ports of the SFP module to keep the optical interfaces clean.

Step 4 Unlock and remove the SFP module, as shown in Figure 2-8.

If the module has a bale-clasp latch, pull the bale out and down to eject the module. If the bale-clasp latch is obstructed and you cannot use your index finger to open it, use a small, flat-blade screwdriver or other long, narrow instrument to open the bale-clasp latch.

Figure 2-8 Removing a Bale-Clasp Latch SFP Module by Using a Flat-Blade Screwdriver



1	Bale clasp

Step 5 Grasp the SFP module between your thumb and index finger, and carefully remove it from the module slot.

Step 6 Place the removed SFP module in an antistatic bag or other protective environment.

Connecting to the 10/100/1000 Ports

The switch 10/100/1000 ports configure themselves to operate at the speed of attached devices. If the attached ports do not support autonegotiation, you can explicitly set the speed and duplex parameters. Connecting devices that do not autonegotiate or that have their speed and duplex parameters manually set can reduce performance or result in no linkage.

To maximize performance, choose one of these methods for configuring the Ethernet ports:

- Let the ports autonegotiate both speed and duplex.
- Set the port speed and duplex parameters on both ends of the connection.

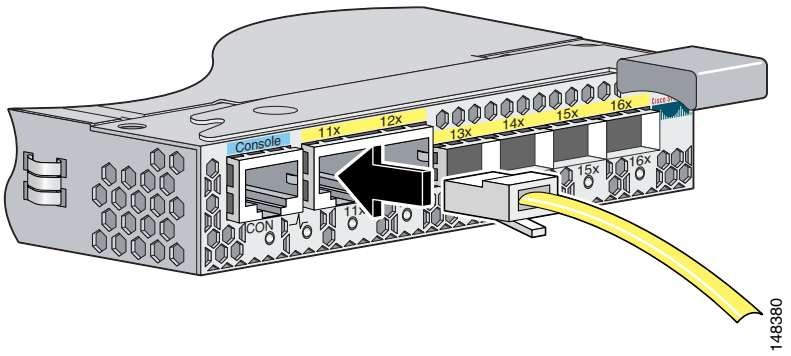
Follow these steps to connect to 10BASE-T, 100BASE-TX or 1000BASE-T devices:

Caution To prevent electrostatic-discharge (ESD) damage, follow your normal board and component handling procedures.

Step 1 When connecting to workstations, servers, routers, and Cisco IP Phones, connect a straight-through cable to an RJ-45 connector on the front panel. (See Figure 2-9.) When connecting to switches or repeaters, use a crossover cable. (See the "Cable and Adapter Specifications" section on page B-4 for cable-pinout descriptions.)

You can use the **mdix auto** interface configuration command in the CLI to enable the automatic medium-dependent interface crossover (auto-MDIX) feature. When the auto-MDIX feature is enabled, the switch detects the required cable type for copper Ethernet connections and configures the interfaces accordingly. Therefore, you can use either a crossover or a straight-through cable for connections to a copper 10/100/1000 or a 1000BASE-T SFP module port on the switch, regardless of the type of device on the other end of the connection. The auto-MDIX feature is enabled by default.

Figure 2-9 Connecting to an Ethernet Port



Note When connecting to 1000BASE-T-compatible devices, be sure to use a twisted four-pair, Category 5 cable.

Step 2 Connect the other end of the cable to an RJ-45 connector on the other device. The port LED turns on when both the switch and the connected device have established link.

The port LED is amber while Spanning Tree Protocol (STP) discovers the topology and searches for loops. This takes about 30 seconds, and then the port LED turns green. If the port LED does not turn on, the device at the other end might not be turned on, or there might be a cable problem or a problem with the adapter installed in the attached device. See Chapter 3, "Troubleshooting," for solutions to cabling problems.

Step 3 Reconfigure and reboot the connected device if necessary.

Step 4 Repeat Steps 1 through 3 to connect each device.

Connecting to SFP Modules

This section describes how to connect to SFP modules. For instructions on how to connect to fiber-optic SFP modules, see the "Connecting to Fiber-Optic SFP Modules" section. For instructions on how to connect to copper 1000BASE-T SFP modules, see the "Connecting to 1000BASE-T SFP Modules" section.

For instructions about how to install or remove an SFP module, see the "Installing and Removing SFP Modules" section on page 2-13.

Connecting to Fiber-Optic SFP Modules

Follow these steps to connect a fiber-optic cable to an SFP module:

Caution Do not remove the rubber plugs from the SFP module port or the rubber caps from the fiber-optic cable until you are ready to connect the cable. The plugs and caps protect the SFP module ports and cables from contamination and ambient light.

Before connecting to the SFP module, be sure that you understand the port and cabling stipulations in the "Installation Guidelines" section on page 2-3 and in the "SFP Module Slots" section on page 1-3. See Appendix B, "Connector and Cable Specifications" for information about the LC on the SFP module.

Step 1 Remove the rubber plugs from the module port and fiber-optic cable, and store them for future use.

Step 2 Insert one end of the fiber-optic cable into the SFP module port (see Figure 2-10).

Step 3 Insert the other cable end into a fiber-optic receptacle on a target device.

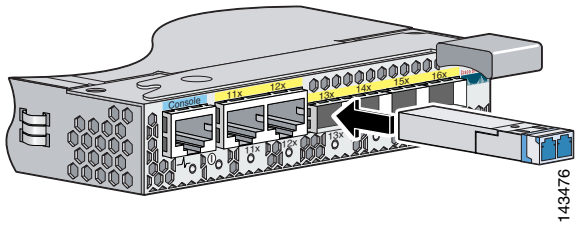
Step 4 Observe the port status LED.

The LED turns green when the switch and the target device have an established link.

The LED turns amber while the STP discovers the network topology and searches for loops. This process takes about 30 seconds, and then the port LED turns green.

If the LED is off, the target device might not be turned on, there might be a cable problem, or there might be a problem with the adapter installed in the target device. See Chapter 3, "Troubleshooting," for solutions to cabling problems.

Figure 2-10 Installing an SFP Module



Step 5 If necessary, reconfigure and restart the switch or target device.

Connecting to 1000BASE-T SFP Modules

Caution To prevent ESD damage, follow your normal board and component handling procedures.

Step 1 When connecting to servers, workstations, and routers, insert a four twisted-pair, straight-through cable in the RJ-45 connector. When connecting to switches or repeaters, insert a four twisted-pair, crossover cable.

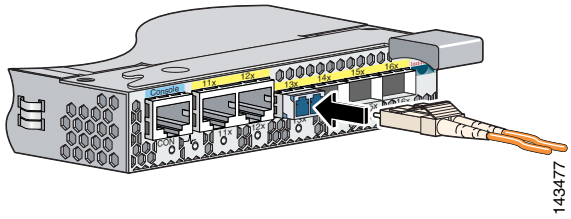
Note When connecting to a 1000BASE-T device, be sure to use a four twisted-pair, Category 5 cable. See Figure 2-7.

Note You can use the **mdix auto** interface configuration command in the CLI to enable the auto-MDIX feature. When the auto-MDIX feature is enabled, the switch detects the required cable type for copper Ethernet connections and configures the interfaces accordingly. Therefore, you can use either a crossover or a straight-through cable for connections to a copper 10/100/1000 or 1000BASE-T SFP module port on the switch, regardless of the type of device on the other end of the connection.

The auto-MDIX feature is enabled by default.

Step 2 Insert the other cable end in an RJ-45 connector on a target device. See Figure 2-11.

Figure 2-11 Inserting the Cable into the SFP Module Port



Step 3 Observe the port status LED.

The LED turns green when the switch and the target device have an established link.

The LED turns amber while the STP discovers the network topology and searches for loops. This process takes about 30 seconds, and then the port LED turns green.

If the LED is off, the target device might not be turned on, there might be a cable problem, or there might be a problem with the adapter installed in the target device. See Chapter 3, "Troubleshooting," for solutions to cabling problems.

Step 4 If necessary, reconfigure and restart the switch or target device.

Where to Go Next

If the default configuration is satisfactory, the switch does not need further configuration. You can use any of these management options to change the default configuration:

- Using the Device Manager

  Access the device manager through a web browser from anywhere in your network. Follow these steps:

  a. Launch a web browser on your PC or workstation.

  b. Enter the switch IP address in the web browser, and press **Enter**. The device manager page appears.

  c. Use the device manager to perform basic switch configuration and monitoring. Refer to the device manager online help for more information.

- Using the Command-Line Interface

  The switch CLI) is based on Cisco IOS software and enhanced to support desktop-switching features. You can fully configure and monitor the switch from the CLI. You can access the CLI either by connecting your management station directly to the switch console port or by using Telnet from a remote management station. Refer to the switch module command reference on Cisco.com for more information.

- Using SNMP

  You can use SNMP management applications such as CiscoWorks. You also can manage the switch from an SNMP-compatible workstation that is running platforms such as SunNet Manager.

Troubleshooting

The LEDs on the front panel provide troubleshooting information about the switch. They show failures in the power-on self-test (POST), port-connectivity problems, and overall switch performance. For a full description of the switch LEDs, see the "LEDs" section on page 1-4.

You can also get statistics from the browser interface, from the command-line interface (CLI), or from a Simple Network Management Protocol (SNMP) workstation. Refer to the software configuration guide, the switch command reference guide on Cisco.com, or the documentation that came with your SNMP application for details.

This chapter describes these topics for troubleshooting problems:

- Understanding POST Results, page 3-1
- Diagnosing Problems, page 3-1

Understanding POST Results

As the switch powers on, it begins the POST, a series of tests that runs automatically to ensure that the switch functions properly. When the POST completes successfully, the System Status/ID LED is off, and the Console LED is solid green or amber. If the switch fails POST because of a misconfiguration or error, the System Status/ID LED blinks green, and the Console LED is off.

Note POST failures are usually fatal. Call Cisco Systems if your switch does not pass POST.

Diagnosing Problems

The LEDs on the front panel provide troubleshooting information about the switch. They show POST failures, port-connectivity problems, and overall switch performance. For a full description of the switch LEDs, see the "LEDs" section on page 1-4.

You can also get statistics from the browser interface, from the CLI, or from an SNMP workstation. Refer to the software configuration guide, the switch command reference guide on Cisco.com, or the documentation that came with your SNMP application for details.

You can access the Technical Support Website (http://www.cisco.com/tac) for a list of known hardware problems and extensive troubleshooting documentation including:

- Field notices
- Security advisories
- Troubleshooting resources
- Factory defaults
- Password recovery
- Recovery from corrupted or missing software
- Switch port problems
- Network interface cards
- Troubleshooting tools

Common switch problems fall into these categories:

- Poor performance
- No connectivity
- Corrupted software

Table 3-1 describes how to detect and resolve these problems.

Table 3-1 Common Problems and Their Solutions

Symptom	Possible Cause	Resolution
Poor performance or excessive errors	Duplex autonegotiation mismatch.	Refer to the switch software configuration guide for information on identifying autonegotiation mismatches.
	Cabling distance exceeded	
	• Port statistics show excessive frame check sequence (FCS), late-collision, or alignment errors.	• Refer to the switch software configuration guide for information on displaying port statistics.
	• For 10/100/1000BASE-T connections:	
	– The distance between the port and the attached device exceeds 328 feet (100 meters).	• Reduce the cable length to within the recommended distances.
	– If the switch is attached to a repeater, the total distance between the two end stations exceeds the cabling guidelines.	• Refer to your repeater documentation for cabling guidelines.
	• For SFP port connections:	• Refer to your SFP documentation for cabling guidelines.
	– The distance between the SFP port and the attached device exceeds the SFP cabling guidelines.	
	Bad adapter in attached device	
	• Excessive errors found in port statistics.	• Run adapter card diagnostic utility.
	• STP checking for possible loops.	• Wait 30 seconds for the port LED to turn green.

Table 3-1 Common Problems and Their Solutions (continued)

Symptom	Possible Cause	Resolution
No connectivity	**Incorrect or bad cable** These are results of no link at both ends: • A crossover cable was used when a straight-through was required, or the reverse.	• For the correct pinouts and the proper application of crossover or straight-through cables, see the "Two Twisted-Pair Cable Pinouts" section on page B-4.
	• The cable is wired incorrectly.	• Replace with a tested good cable.
	• A crossover or straight-through cable is wired incorrectly.	• For 1000BASE-T connections, be sure to use a twisted four-pair, Category 5 cable.
	• STP checking for possible loops.	• Wait 30 seconds for the port LED to turn green.
Unreadable characters on the management console	Incorrect baud rate.	Reset the emulation software to 9600 baud.
Amber system LED	Fatal POST error detected.	Contact Cisco Systems.
The switch port is placed in error-disabled state after SFP module is inserted	Bad or non-Cisco-approved SFP module.	Remove the SFP module from the switch, and replace it with a Cisco-approved module. Use the **errdisable recovery cause gbic-invalid** global configuration command to verify the port status, and enter a time interval to recover from the error-disable state. Refer to the switch command reference guide for information on the **errdisable recovery** command.

Table 3-1 Common Problems and Their Solutions (continued)

Symptom	Possible Cause	Resolution
Switch does not recognize the SFP module	The SFP module might be installed upside down. The SFP module does not snap into the slot.	Verify that the SFP module is not installed upside down. Remove the SFP module. Inspect for physical damage to the connector, the module, and the module slot. Replace the SFP module with a known good SFP module.
The switch port is placed in error-disabled state after SFP is inserted	Bad or non-Cisco-approved SFP.	Remove the SFP module from the switch, and replace it with a Cisco-approved module. Use the **errdisable recovery cause gbic-invalid** global configuration command to verify the port status, and enter a time interval to recover from the error-disable state. Refer to the switch command reference guide for information on the **errdisable recovery** command.

Technical Specifications

This appendix lists the switch technical specifications in Table A-1.

Table A-1 Technical Specifications for the Cisco Ethernet Access Switch Module for the Dell Server Chassis

Environmental Ranges	
Operating temperature	32 to 113°F (0 to 45°C)
Storage temperature	–4 to 158°F (–20 to 70°C)
Relative humidity	10 to 90% (noncondensing)
Storage relative humidity	10 to 95% (noncondensing)
Operating altitude	10,000 feet (3048 meters)
Storage altitude	15,000 feet (4572 meters)
Physical Dimensions	
Weight	2 lbs (0.90 kg)
Dimensions (H x D x W)	1.35 x 5.12 x 10.93 in. (3.4 x 13 x 27.8 cm)

See the *Regulatory Compliance and Safety Information for the Cisco Catalyst Blade Switch 3030* guide for information about safety compliance and electromagnetic compatibility.

Connector and Cable Specifications

This appendix describes the switch module ports and the cables and adapters that you use to connect the switch to other devices.

Connector Specifications

These sections describe the connectors used with the switch module.

10/100/1000 Ports

The 10/100/1000 Ethernet ports on the switch use standard RJ-45 connectors. Figure B-1 shows the pinout.

Note You can use the **mdix auto** interface configuration command in the CLI to enable the automatic medium-dependent interface crossover (auto-MDIX) feature. When the auto-MDIX feature is enabled, the switch detects the required cable type for copper Ethernet connections and configures the interfaces accordingly. Therefore, you can use either a crossover or a straight-through cable for connections to a copper 10/100/1000 or 1000BASE-T SFP module port on the switch, regardless of the type of device on the other end of the connection.

The auto-MDIX feature is enabled by default on switches running Cisco IOS Release 12.2(18)SE or later. For releases between Cisco IOS Release 12.1(14)EA1 and 12.2(18)SE, the auto-MDIX feature is disabled by default. For configuration information for this feature, refer to the switch software configuration guide or the switch command reference.

Connecting to 10BASE-T- and 100BASE-TX-Compatible Devices

When connecting the ports to 10BASE-T- and 100BASE-TX-compatible devices, such as servers, workstations, and routers, you can use a two or four twisted-pair, straight-through cable wired for 10BASE-T and 100BASE-TX. Figure B-4 shows the two twisted-pair, straight-through cable schematics. Figure B-6 shows the four twisted-pair, straight-through cable schematics.

When connecting the ports to 10BASE-T- and 100BASE-TX-compatible devices, such as switches or repeaters, you can use a two or four twisted-pair, crossover cable. Figure B-5 shows the two twisted-pair, crossover cable schematics. Figure B-7 shows the four twisted-pair, crossover cable schematics.

You can use Category 3, 4, or 5 cabling when connecting to 10BASE-T-compatible devices. You must use Category 5 cabling when connecting to 100BASE-TX-compatible devices.

Connecting to 1000BASE-T Devices

When connecting the ports to 1000BASE-T devices, such as servers, workstations, and routers, you must use a four twisted-pair, Category 5, straight-through cable wired for 10BASE-T, 100BASE-TX, and 1000BASE-T. Figure B-6 shows the straight-through cable schematics.

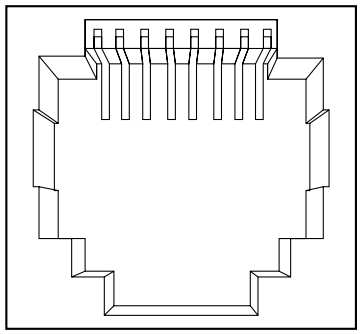
When connecting the ports to other devices, such as switches or repeaters, you must use a four twisted-pair, Category 5, crossover cable. Figure B-7 shows the crossover cable schematics.

Note Be sure to use a four twisted-pair, Category 5 cable when connecting to a 1000BASE-T-compatible device.

Note Use a straight-through cable to connect two ports only when one port is designated with an X. Use a crossover cable to connect two ports when both ports are designated with an X or when both ports do not have an **X**.

Figure B-1 10/100/1000 Port Pinouts

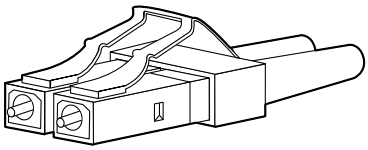
Pin	Label
1	TP0+
2	TP0-
3	TP1+
4	TP2+
5	TP2-
6	TP1-
7	TP3+
8	TP3-



SFP Module Ports

The switch uses SFP modules for fiber-optic and copper uplink ports. Refer to the release notes for a list of supported SFP modules.

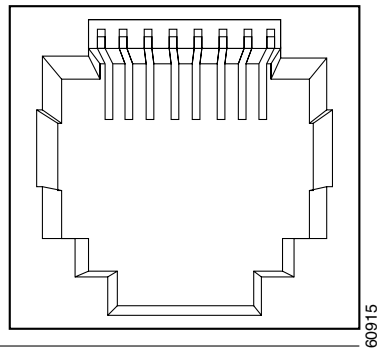
Figure B-2 Fiber-Optic SFP Module LC Connector



Warning **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.** Statement 1051

Figure B-3 Copper SFP Module RJ-45 Connector

Pin	Label
1	TP0+
2	TP0-
3	TP1+
4	TP2+
5	TP2-
6	TP1-
7	TP3+
8	TP3-



Console Port

The console port uses an 8-pin RJ-45 connector, which is described in Table B-1 and Table B-2. The supplied RJ-45-to-DB-9 adapter cable is used to connect the console port of the switch to a console PC. You need to provide a RJ-45-to-DB-25 female DTE adapter if you want to connect the switch console port to a terminal. You can order a kit (part number ACS-DSBUASYN=) containing that adapter from Cisco. For console port and adapter pinout information, see Table B-1 and Table B-2.

Cable and Adapter Specifications

These sections describe the cables and adapters used with the switch.

Two Twisted-Pair Cable Pinouts

Figure B-4 and Figure B-5 show the schematics of two twisted-pair cables for connecting to 10BASE-T- and 100BASE-TX-compatible devices.

Figure B-4 Two Twisted-Pair Straight-Through Cable Schematic

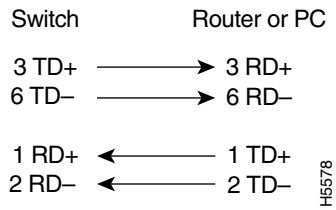
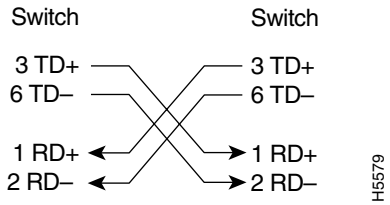


Figure B-5 Two Twisted-Pair Crossover Cable Schematic



Four Twisted-Pair Cable Pinouts for 1000BASE-T Ports

Figure B-6 and Figure B-7 show the schematics of four twisted-pair cables for 10/100/1000 ports on the switch.

Figure B-6 Four Twisted-Pair Straight-Through Cable Schematic for 10/100/1000 Ports

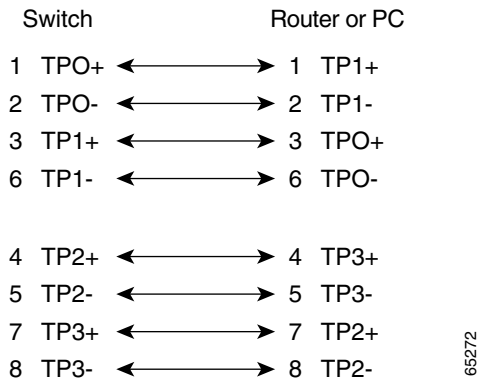
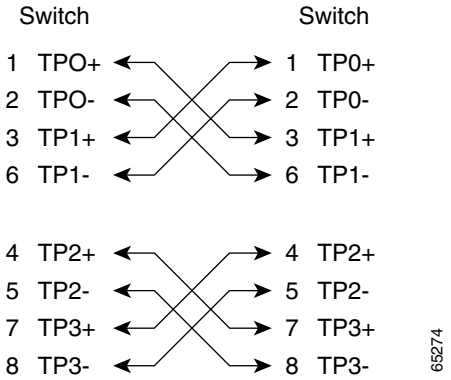


Figure B-7 Four Twisted-Pair Crossover Cable Schematics for 10/100/1000 Ports



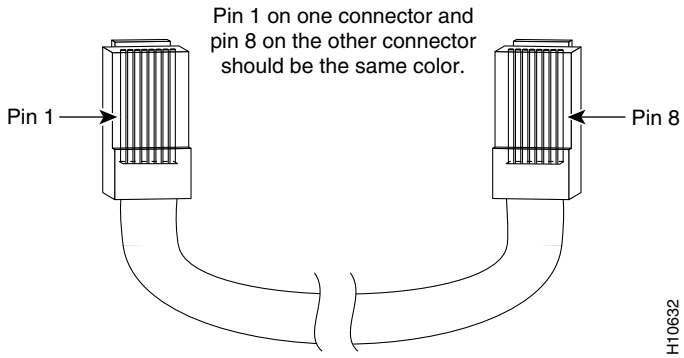
Crossover Cable and Adapter Pinouts

This section describes how to identify a crossover cable and also describes the adapter pinouts.

Identifying a Crossover Cable

To identify a crossover cable, compare the two modular ends of the cable. Hold the cable ends side-by-side, with the tab at the back. The wire connected to the pin on the outside of the left plug should be the same color as the wire connected to the pin on the outside of the right plug. (See Figure B-8.)

Figure B-8 Identifying a Crossover Cable



Adapter Pinouts

Table B-1 lists the pinouts for the console port, the RJ-45-to-DB-9 adapter cable, and the console device.

Table B-1 Console Port Signaling Using a DB-9 Adapter

Switch Console Port (DTE)	RJ-45-to-DB-9 Terminal Adapter	Console Device
Signal	**DB-9 Pin**	**Signal**
RTS	8	CTS
DTR	6	DSR
TxD	2	RxD
GND	5	GND
GND	5	GND
RxD	3	TxD
DSR	4	DTR
CTS	7	RTS

Table B-2 lists the pinouts for the console port, RJ-45-to-DB-25 female DTE adapter, and the console device.

Note The RJ-45-to-DB-25 female DTE adapter is not supplied with the switch. You can order a kit (part number ACS-DSBUASYN=) containing this adapter from Cisco.

Table B-2 Console Port Signaling Using a DB-25 Adapter

Switch Console Port (DTE)	RJ-45-to-DB-25 Terminal Adapter	Console Device
Signal	**DB-25 Pin**	**Signal**
RTS	5	CTS
DTR	6	DSR
TxD	3	RxD
GND	7	GND
GND	7	GND
RxD	2	TxD
DSR	20	DTR
CTS	4	RTS

Configuring the Switch with the CLI-Based Setup Program

This chapter provides a quick installation and setup procedure for the switch.

Note For detailed installation procedures, see Chapter 2, "Switch Installation." For product overview information, see Chapter 1, "Product Overview."

These steps describe how to do a simple installation:

1. Accessing the CLI Through the Console Port, page C-1
2. Taking Out What You Need, page C-1
3. Connecting to the Console Port, page C-2
4. Completing the Initial Configuration, page C-4

Accessing the CLI Through the Console Port

You can access the CLI on a configured or unconfigured switch by connecting the console port of the switch to the serial port on your PC or workstation and accessing the switch through a Telnet session.

Taking Out What You Need

These items ship with your switch module:

- Console cable
- *Cisco Catalyst Blade Switch 3030 Getting Started Guide*
- *Regulatory Compliance and Safety Information for the Cisco Catalyst Blade Switch 3030*
- Registration card

Follow these steps:

1. Unpack and remove the switch module and the accessory kit from the shipping box.
2. Return the packing material to the shipping container, and save it for future use.

Note If the switch modules are ordered with the server chassis, the switch modules are already installed, and no unpacking is required. The unpacking procedure applies only if a switch module is ordered separately.

Note You need to provide the Category 5 straight-through cables to connect the switch ports to other Ethernet devices.

Note You can use the **mdix auto** interface configuration command in the CLI to enable the automatic medium-dependent interface crossover (auto-MDIX) feature. When the auto-MDIX feature is enabled, the switch detects the required cable type for copper Ethernet connections and configures the interfaces accordingly. Therefore, you can use either a crossover or a straight-through cable for connections to a copper 10/100/1000 or 1000BASE-T SFP module port on the switch, regardless of the type of device on the other end of the connection.

The auto-MDIX feature is enabled by default on switches running Cisco IOS Release 12.2(18)SE or later. For releases between Cisco IOS Release 12.1(14)EA1 and 12.2(18)SE, the auto-MDIX feature is disabled by default. For configuration information for this feature, refer to the switch software configuration guide or the switch command reference.

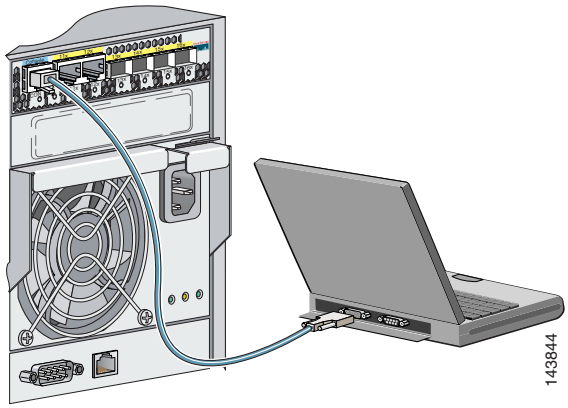
Connecting to the Console Port

Obtain and make note of this information from your network administrator before you begin the switch module installation:

- Switch IP address
- Subnet mask (IP netmask)
- Default gateway (router)
- Enable secret password (encrypted)
- Enable password (not encrypted)
- Telnet password
- SNMP community strings (optional)

Step 1 Connect one end of the console cable to the switch module console port. Connect the other end of the cable to the serial port of the computer that is running the terminal emulation application. (See Figure C-1.)

Figure C-1 Connecting through the Switch Module Console Port



Step 2 Start the terminal emulation session so that you can see the output display from the power-on self-test (POST). The terminal-emulation software—a PC application such as Hyperterminal or ProcommPlus—makes communication between the switch and your PC or terminal possible.

Configure the baud rate and character format of the PC or terminal to match these console port default characteristics:

- 9600 baud
- 8 data bits
- 1 stop bit
- No parity
- None (flow control)

Step 3 Wait for the switch to complete the POST. It might take several minutes for the switch to complete POST.

Step 4 Verify that POST has completed by confirming that the System Status/ID LED is off and that the Console LED is solid green or amber. If the switch fails POST because of a misconfiguration or error, the System Status/ID LED blinks green, and the Console LED is off.

Log into the DRAC/MC console to get more details about the failure mode.

POST errors are usually fatal. Call Cisco Customer Support immediately if your switch fails POST.

See item 4 in Figure 1-1 on page 1-2 for the location of the System Status/ID LED and the Console LED.

Step 5 Wait for the switch to complete flash initialization. When you see the prompt, ***Press Return to Get Started!***, press **Return** or **Enter**.

Step 6 Make sure that the System Status/ID LED on the switch module is off and that the Console LED is green or amber. This means that the switch module is operating properly.

Step 7 See the "Completing the Initial Configuration" section on page C-4 for instructions on setting up and initially configuring the switch module.

Completing the Initial Configuration

Follow these steps to complete the setup program and to create an initial configuration for the switch.

Note For information about automatically configuring the switch, see the "Assigning the Switch IP Address and Default Gateway" chapter in the switch configuration guide.

Step 1 After you have pressed **Enter** or **Return** after the prompt to start the initial configuration setup program, enter **yes** at these prompts:

```
Would you like to terminate autoinstall? [yes]: yes
--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: yes

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:
```

Step 2 Enter a hostname for the switch after the prompt, and press **Return**.

The hostname is limited to 20 characters. Do not use *-n*, where n is a number, as the last character in a hostname for any switch.

Step 3 Enter an enable secret password, and press **Return**.

The password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, allows spaces, but ignores leading spaces. The secret password is encrypted, and the enable password is in plain text.

Step 4 Enter an enable password, and press **Return**.

Step 5 Enter a virtual terminal (Telnet) password, and press **Return**.

The password can be from 1 to 25 alphanumeric characters, is case sensitive, allows spaces, but ignores leading spaces.

Step 6 (Optional) Configure Simple Network Management Protocol (SNMP) by responding to the prompts.

1. To configure SNMP later, press **Return** (which applies the default of no). If you accept the default, you can configure SNMP later through the CLI.

   ```
   Configure SNMP Network Management? [no]:
   ```

2. To configure SNMP now, enter **yes**.

   ```
   Configure SNMP Network Management? [no]: yes
   Community string [public]: public
   ```

Step 7 Enter the interface name (physical interface or VLAN name) of the interface that connects to the management network, and press **Return**.

Enter **vlan1** for the interface name at this prompt.

Step 8 To configure the interface, enter **Yes** after the prompt, and then enter the switch IP address and subnet mask. Press **Return**.

The IP address and subnet mask shown here are examples:

```
Configuring interface Vlan1:
Configure IP on this interface? [yes]:
IP address for this interface [10.0.0.1]:
Subnet mask for this interface [255.255.255.0] : 255.255.255.0
Class A network is 10.0.0.1, 21 subnet bits; mask is /21
```

Step 9 Enter **no** when the prompt asks you if you would like to enable the switch as a cluster command switch. This switch will be a standalone switch.

```
Would you like to enable as a cluster command switch? [yes/no]: no
```

Note Clustering is not supported on the Cisco Catalyst Blade Switch 3030.

You have now completed the initial configuration of the switch, and the switch displays its initial configuration. An example of the output is shown here:

```
The following configuration command script was created:
hostname switch1
enable secret 5 $1$cagJ$e4LP91PNazfdADoNAZm6y0
enable password enable_password
line vty 0 15
password terminal-password
snmp-server community public
!
!
interface Vlan1
no shutdown
ip address 10.0.0.1 255.255.255.0
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2

. . . (output truncated)



interface GigabitEthernet0/16
!
end
```

Step 10 These choices appear:

```
[0] Go to the IOS command prompt without saving this config.

[1] Return back to the setup without saving this config.

[2] Save this configuration to nvram and exit.

If you want to save the configuration and use it the next time the switch reboots, save it
in NVRAM by selecting option 2.

Enter your selection [2]:2
```

Make your selection, and press **Return**.

Step 11 Disconnect the server chassis serial port or the switch console port from the PC. See the "Management Options" section on page 1-6 for information about managing the switch.

Numerics

10/100/1000 ports
  cable lengths 2-3
  connecting to 2-16
  connectors and cables B-1 to B-2
  description 1-3
  illustrated 1-2
1000BASE-T SFP module cable lengths 2-3

A

adapter pinouts, terminal
  RJ-45-to-DB-25 B-6
  RJ-45-to-DB-9 B-6
auto-MDIX 1-3, 2-16, 2-18, B-1, C-2
autonegotiation 1-3

C

cable lengths 2-3
cables
  crossover
    connecting to B-2
    four twisted-pair pinout, 1000BASE-T ports B-5
    identifying B-5
    two twisted-pair pinout, 10/100 ports B-4
  SFP module
    1000BASE-T module 2-18
  straight-through
    connecting to B-1
    four twisted-pair pinout, 1000BASE-T ports B-4
    two twisted-pair pinout B-4
cabling
  10/100/1000 ports 1-3, 2-16
  auto-MDIX 1-3, 2-16, 2-18, B-1, C-2
  pinouts B-4
  See also connectors and cables
cautions viii
Cisco IOS command-line interface 1-7, 2-19
Cisco IP Phones, connecting to 2-16
Class 1 laser warning 2-2
CLI 1-7, 2-19
  accessing through console port 2-8, C-1
command-line interface
  See CLI
configuration examples, network 1-1
connecting
  to 10/100/1000 ports 2-16
  to console port B-3
  to SFP modules 2-17 to 2-19
connection procedures 2-16 to 2-19
connectivity problems, solving 3-2
connectors and cables
  10/100/1000 ports B-1 to B-2
  console port B-3 to B-6
  SC connectors B-3
  SFP module ports B-3
console port
  connectors and cables B-3 to B-6
  description 1-2
console port LED
  description 1-4
  location 1-2
  showing that POST is complete 2-11
conventions, document viii

crossover cable B-5
connecting to 1000BASE-T SFP module ports 2-18
connectivity problems 3-4
pinout
four twisted-pair, 1000BASE-T ports B-5

D

Dell Remote Access Controller/Modular Chassis
See DRAC/MC
device manager
description 1-6
how to access 2-19
diagnosing problems 3-2
disposal of product warning 2-2
document conventions viii
DRAC/MC
accessing through the console serial port 2-9
CLI 2-10
location 2-5

E

electrical codes warning 2-3
electrical noise, avoiding 2-4
Ethernet cable shielding warning 2-2
Ethernet port connections warning 2-3
examples, network configuration 1-1

F

fan 1-4
features 1-1 to 1-2
front panel
10/100 /1000 ports 1-3
description 1-2
LEDs 1-4 to 1-5
SFP module ports 1-3

G

grounded equipment warning 2-2

I

installation
See also procedures
installation instructions warning 2-2
installing SFP module 2-14

J

jewelry removal warning 2-2

L

laser radiation warning B-3
LC connector B-3
LEDs
console port 1-4
port 1-5
POST results 2-11, 3-1
system status 1-4
troubleshooting with 3-1
lightning activity warning 2-2

M

managing the switch
using device manager 1-6
using SNMP 1-7, 2-19
using the CLI 1-7, 2-19
module temperature control 1-4

N

network configuration examples 1-1
noise, electrical 2-4

O

overheating prevention warning 2-2

P

packing list 2-4
performance problems, solving 3-2
pinouts
  10/100 ports B-3
  adapters B-5
  console port B-6, B-6
  crossover cable B-5
  crossover cables
    four twisted-pair, 1000BASE-T ports B-5
    two twisted-pair 10/100 ports B-4
  RJ-45-to-DB-25 terminal adapter B-6
  RJ-45-to-DB-9 terminal adapter B-6
  SFP module ports B-3
  straight-through cables
    four twisted-pair 1000BASE-T ports B-4
    two twisted-pair B-4
port LEDs 1-5
ports
  10/100/1000 1-2, 1-3
  numbering of 10/100/1000 1-3
POST
  completion 2-11
  LEDs 3-1
  results 2-11, 3-1
 power-on self test
  See POST
procedures
  connection 2-16 to 2-19
  installation 2-6 to 2-13
publications, related xiii

R

rear panel description 1-5
release latch location 1-2
removing SFP modules 2-15
restricted access areas warning 2-2
RJ-45 connector, console port B-3

S

safety 2-1
server chassis
  architecture 2-5
  description 2-1
SFP modules
  bale-clasp latch removal 2-15
  connecting to 2-17 to 2-19
  connectors B-3
  description 1-3
  installation 2-14
software switch management 1-6
specifications A-1
straight-through cable
  pinout
    four twisted-pair 1000BASE-T ports B-4
    two twisted-pair 10/100 ports B-4
system LED
  See system status/ID LED
system status/ID LED
  description 1-4
  location 1-2
  showing that POST is complete 2-11

T

technical specifications A-1
Telnet, and accessing the CLI 1-7, 2-19
temperature, operating A-1
temperature monitor 1-4
trained and qualified personnel warning 2-2
troubleshooting 3-1 to 3-4

U

using the CLI to manage the switch 1-7, 2-19

W

warnings
  Class 1 laser 2-2
  defined viii
  disposal of product 2-2
  electrical codes 2-3
  Ethernet cable shielding 2-2
  Ethernet port connections 2-3
  grounded equipment 2-2
  installation 2-1
  installation instructions 2-2
  jewelry removal 2-2
  laser radiation B-3
  lightning activity 2-2
  overheating prevention 2-2
  restricted access areas 2-2
  trained and qualified personnel 2-2